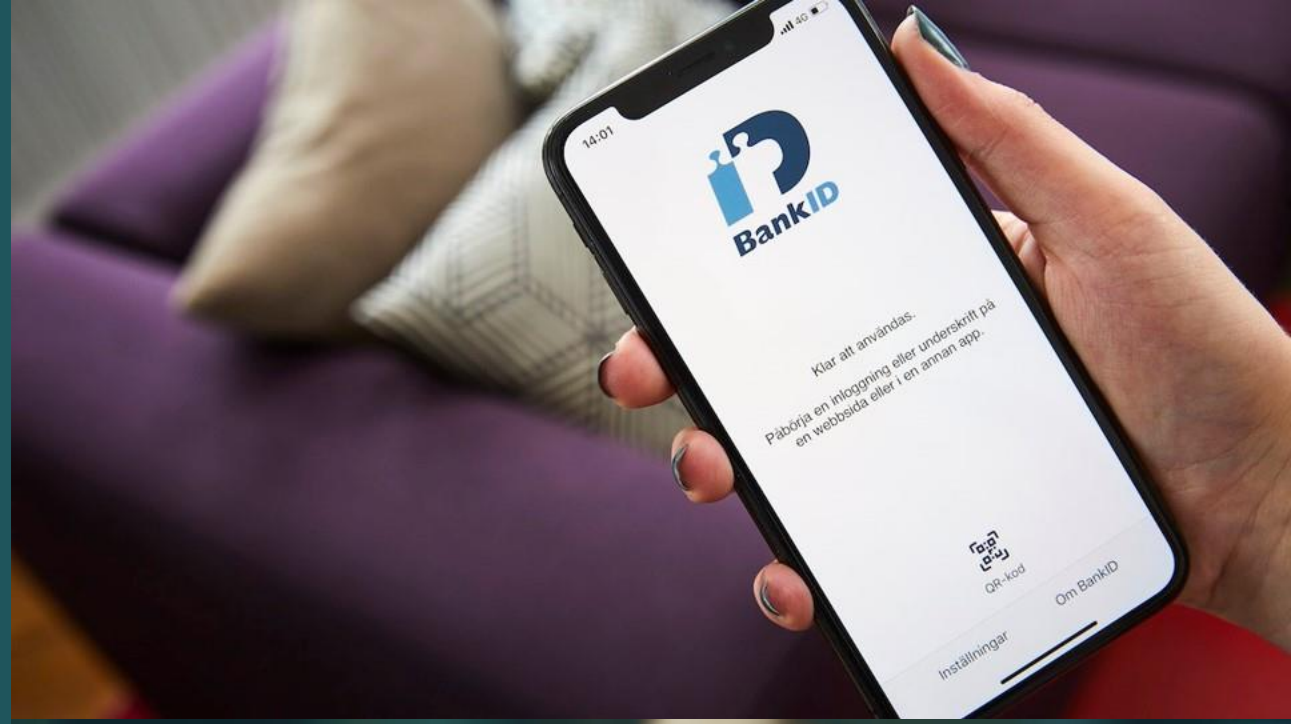
Digitala brott mot företag & företagare

Cyberdagen i Linköping 2023-10-10

Pontus Lindström, brott- och säkerhetsexpert
Företagarnaföret



SVERIGE

Cyberattack mot it-företaget Softronic – a-kassor ligger nere

UPPDATERAD 2022-12-02 PUBLICERAD 2022-12-02

It-systemet för Sveriges 24 a-kassor låg på fredagen nere på grund av en hackerattack. Foto: Thomas Karlsson

Flera viktiga it-system, bland annat samtliga svenska a-kassor, har slagits ut eller stängts efter en cyberattack mot it-företaget Softronic. A-kassornas webbtjänster hålls tills vidare stängda och kommer tidigast starta under helgen.

Cyberangrepp tvingar Norrköping att förbereda sig för it-stopp

Publicerad: 5 december 2022, 12:44

"Fortfarande stor risk att it-miljön går ner", säger Anna Selander, tillförordnad kommundirektör.
Foto: Pressbild/Norrköpings kommun

En pågående it-attack gör att Norrköpings kommun är i stabsläge. Kommunens anställda förbereder sig nu på att kunna gå över från dator till att arbeta med papper och penna.

företagarna

Ryska hackers misstänks ligga bakom it-attacken i Kalix. **Foto: SVT**

Efter it-attacken i Kalix riktas misstankar mot Ryssland

UPPDATERAD 19 JANUARI 2022 PUBLICERAD 19 JANUARI 2022

Ryska hackers misstänks ligga bakom it-attacken i Kalix, vilket P4 Norrbotten är först med att rapportera.

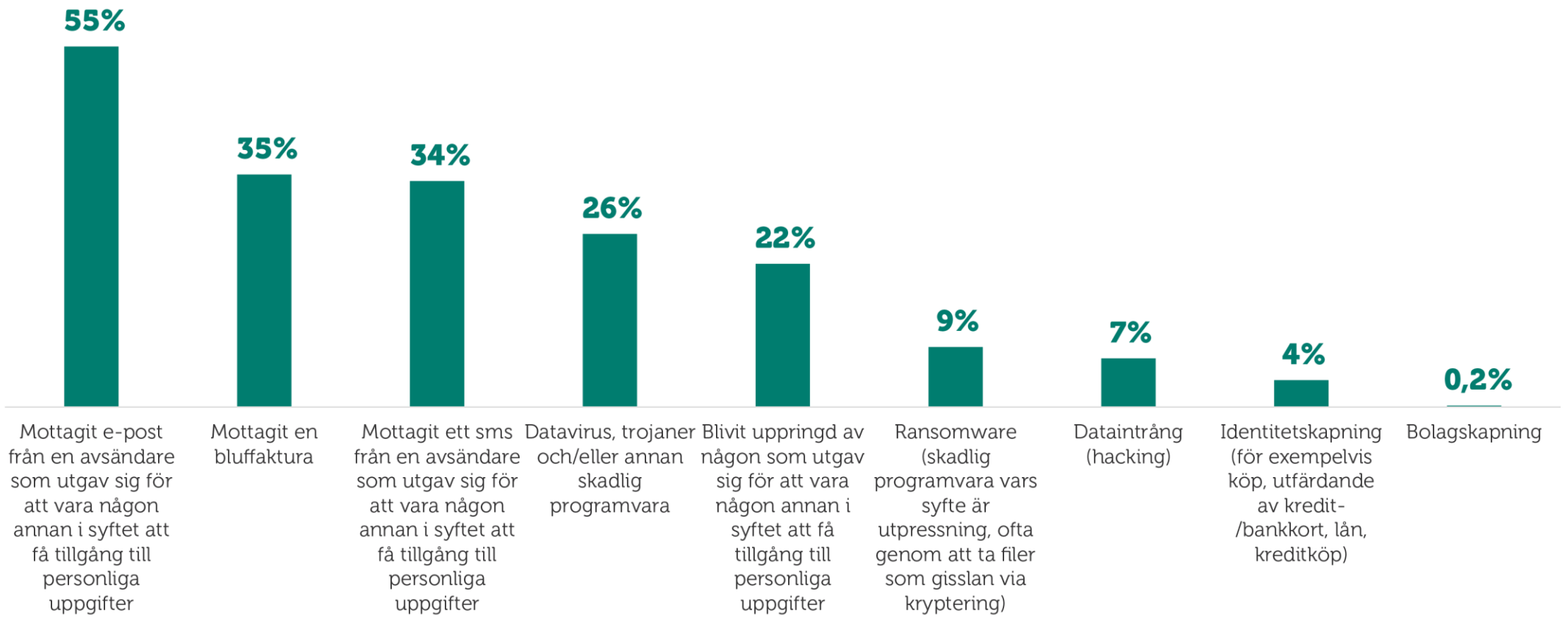
”Hackergrupperna funkar nästan som företag” hör SVT:s tech-korrespondent Alexander Norén om hackerattacken. **Foto: SVT**

Coop-butiker hölls stängda under helgen – inget besked för måndag

UPPDATERAD 5 JULI 2021 PUBLICERAD 4 JULI 2021


Bolagsverket
Konsument verket · KO
Sveriges Kommuner och Regioner
Statens servicecenter
IMY. Integritetsskydds myndigheten
SSF Stöldskyddsföreningen
SVENSKT NÄRINGSLIV
PENSIONS MYNDIGHETEN
företagarna
Verksamt.se Till företag från myndigheter
Handelsbanken
TÄNK SÄKERT
Nordea
Konsumenternas
MYNDIGHETEN FÖR DIGITAL FÖRVALTNING Agency for Digital Government
Polisen
MSB Myndigheten för samhällsskydd och beredskap
ISACA Sweden Chapter
DATAFÖRENINGEN Digital destination Sverige
Telia
SäkerhetsBranschen KUNSKAP · ANSVAR · KVALITET
SACS Swedish Association of Civil Security
Skatteverket
SH Svensk Handel
INTERNET STIFTELSEN

Digitala brott som drabbar företagare



Bas: Samtliga företag, n=1216

företagarna

Exempel phishing (nätfiske)

Från: Företagarna ProSurvey <info@foretagarna.se.sbdc.nu>
Skickat: den 7 mars 2023 12:07
Till: Pontus Lindström <pontus.lindstrom@foretagarna.se>
Ämne: Företagarna Medarbetarundersökning

The generic COMAPANY

Företagarna Medarbetarundersökning

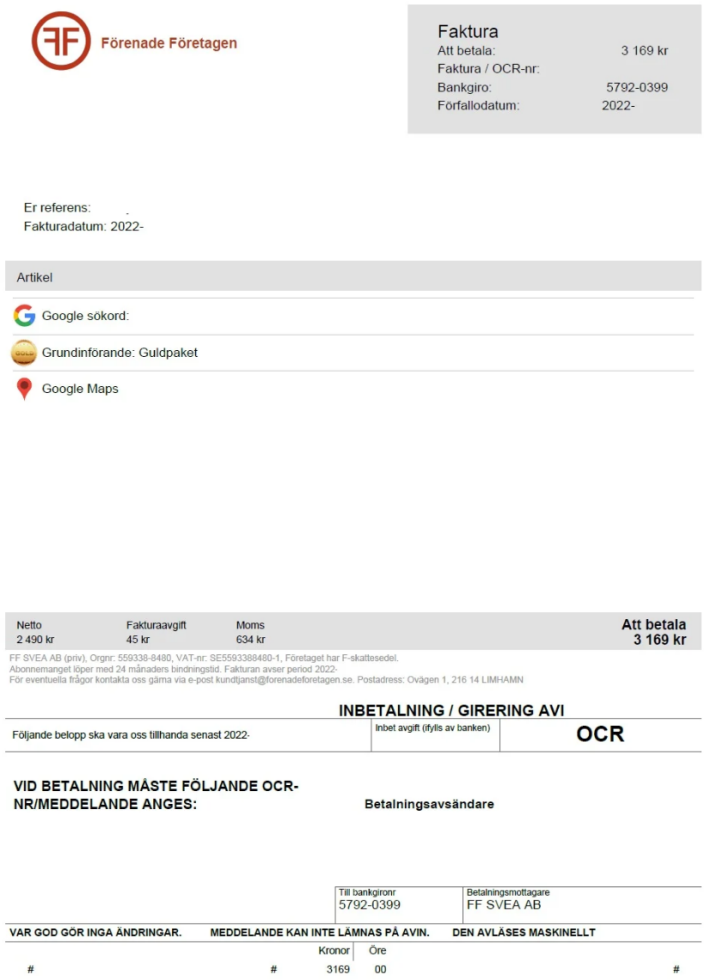
Nu genomför vi en kort medarbetarundersökning för att förbättra arbetsmiljö och säkerhet på Företagarna. Alla medarbetare ombedes besvara 10 frågor före tisdag nästa vecka.

Du finner frågeformuläret på följande länk: Medarbetarundersökning Formulär

Vi använder verktyget ProSurvey för att samla in dina svar. Använd dina vanliga inloggningsuppgifter om du ombeds logga in.

Exempel smishing (sms)

Exempel bluffakturor



Förenade Företagen

Faktura
Att betala: 3 169 kr
Faktura / OCR-nr:
Bankgiro: 5792-0399
Förfallodatum: 2022-

Er referens:
Fakturadatum: 2022-

Artikel
Google sökord:
Grundinförande: Guldpaket
Google Maps

Netto	Fakturaavgift	Moms	Att betala
2 490 kr	45 kr	634 kr	3 169 kr

FF SVEA AB (priv), Orgnr: 559338-8480, VAT-nr: SE5593388480-1, Företaget har F-skattesedel.
Abonnemanget löper med 24 månaders bindningstid. Fakturan avser period 2022-
För eventuella frågor kontakta oss gärna via e-post kundtjanst@forenadeforetagen.se. Postadress: Ovägen 1, 216 14 LIMHAMN

INBETALNING / GIRERING AVI

Följande belopp ska vara oss tillhanda senast 2022-

Inbet avgift (ifylls av banken)

OCR

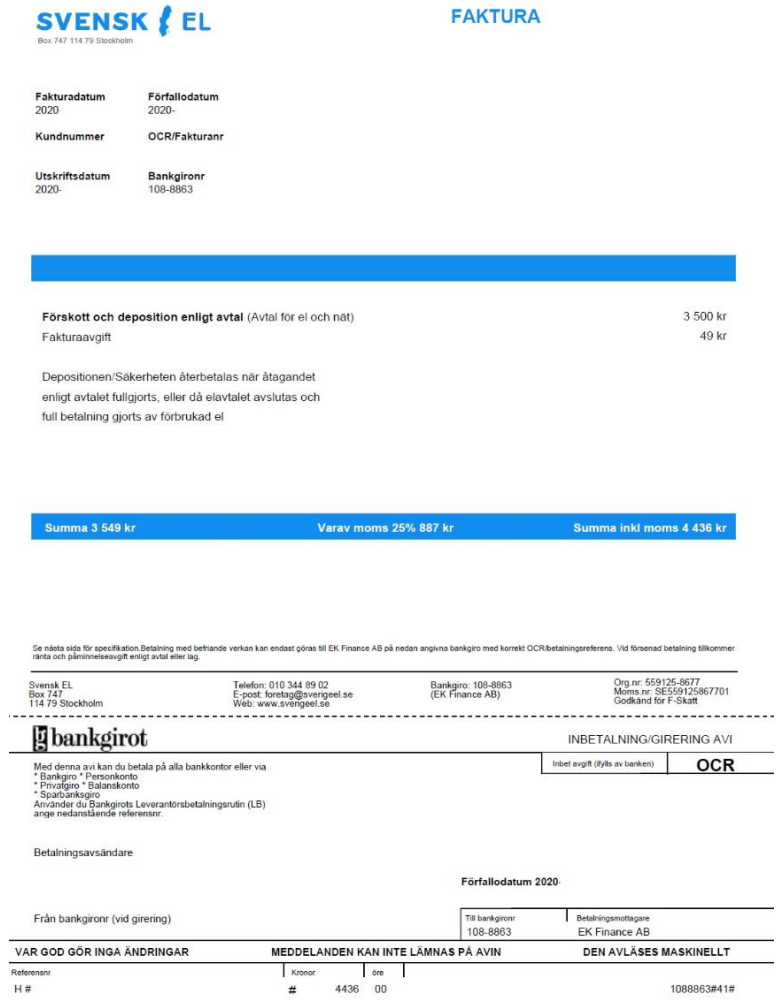
VID BETALNING MÅSTE FÖLJANDE OCR-NR/MEDDELANDE ANGES:

Betalningsavsändare

Till bankgironr	Betalningsmottagare
5792-0399	FF SVEA AB

VAR GOD GÖR INGA ÄNDRINGAR. MEDDELANDE KAN INTE LÄMNAS PÅ AVIN. DEN AVLÄSES MASKINELLT

		Kronor	Öre	
#	#	3169	00	#



SVENSK EL
Box 747 114 79 Stockholm

FAKTURA

Fakturadatum	Förfallodatum
2020	2020-
Kundnummer	**OCR/Fakturanr**
Utskriftsdatum	**Bankgironr**
2020-	108-8863

Förskott och deposition enligt avtal (Avtal för el och nät)	3 500 kr
Fakturaavgift	49 kr

Depositionen/Säkerheten återbetalas när åtagandet enligt avtalet fullgjorts, eller då elavtalet avslutas och full betalning gjorts av förbrukad el

Summa 3 549 kr **Varav moms 25% 887 kr** **Summa inkl moms 4 436 kr**

Se nästa sida för specifikation.Betalning med befriande verkan kan endast göras till EK Finance AB på nedan angivna bankgiro med korrekt OCR/betalningsreferens. Vid försenad betalning tillkommer ränta och påminnelseavgift enligt avtal eller lag.

Svensk EL Box 747 114 79 Stockholm	Telefon: 010 344 89 02 E-post: foretag@svengeel.se Web: www.svengeel.se	Bankgiro: 108-8863 (EK Finance AB)	Org.nr: 559125-8677 Moms.nr: SE559125867701 Godkänd för F-Skatt

bankgirot

INBETALNING/GIRERING AVI

Inbet avgift (ifylls av banken) **OCR**

Med denna avi kan du betala på alla bankkontor eller via
* Bankgiro * Personkonto
* Privatgiro * Balanskonto
* Sparbanksgiro
Använder du Bankgirots Leverantörsbetalningsrutin (LB) ange nedanstående referensnr.

Betalningsavsändare

Förfallodatum 2020-

Från bankgironr (vid girering)

Till bankgironr	Betalningsmottagare
108-8863	EK Finance AB

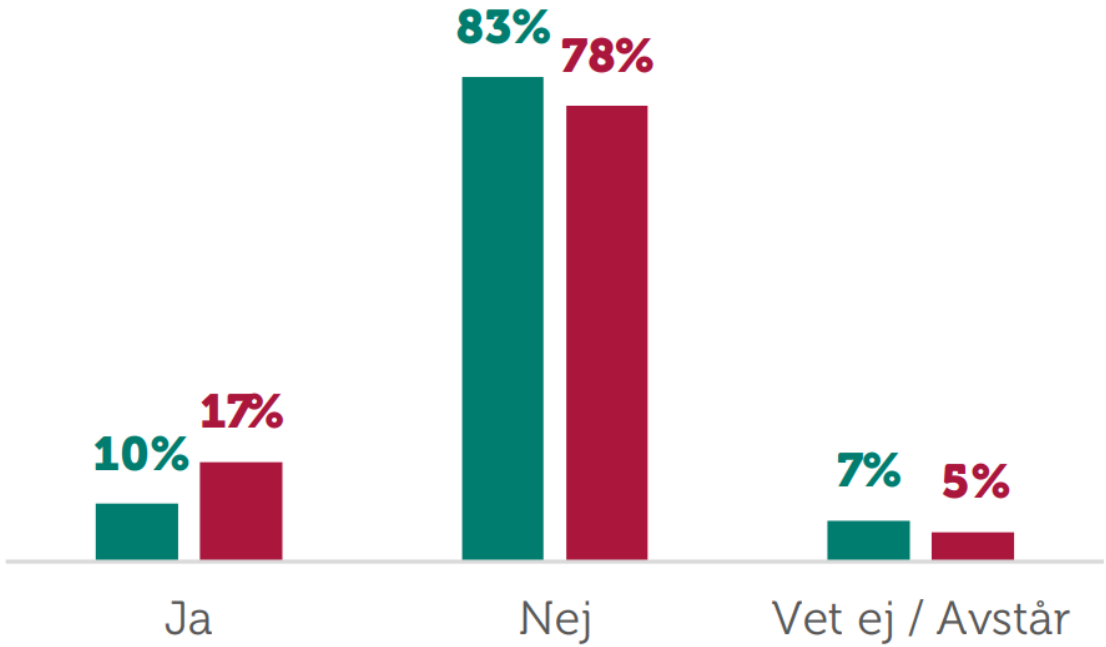
VAR GOD GÖR INGA ÄNDRINGAR MEDDELANDEN KAN INTE LÄMNAS PÅ AVIN DEN AVLÄSES MASKINELLT

Referensnr	Kronor	öre	
H #	# 4436	00	108863#41#

företagarna

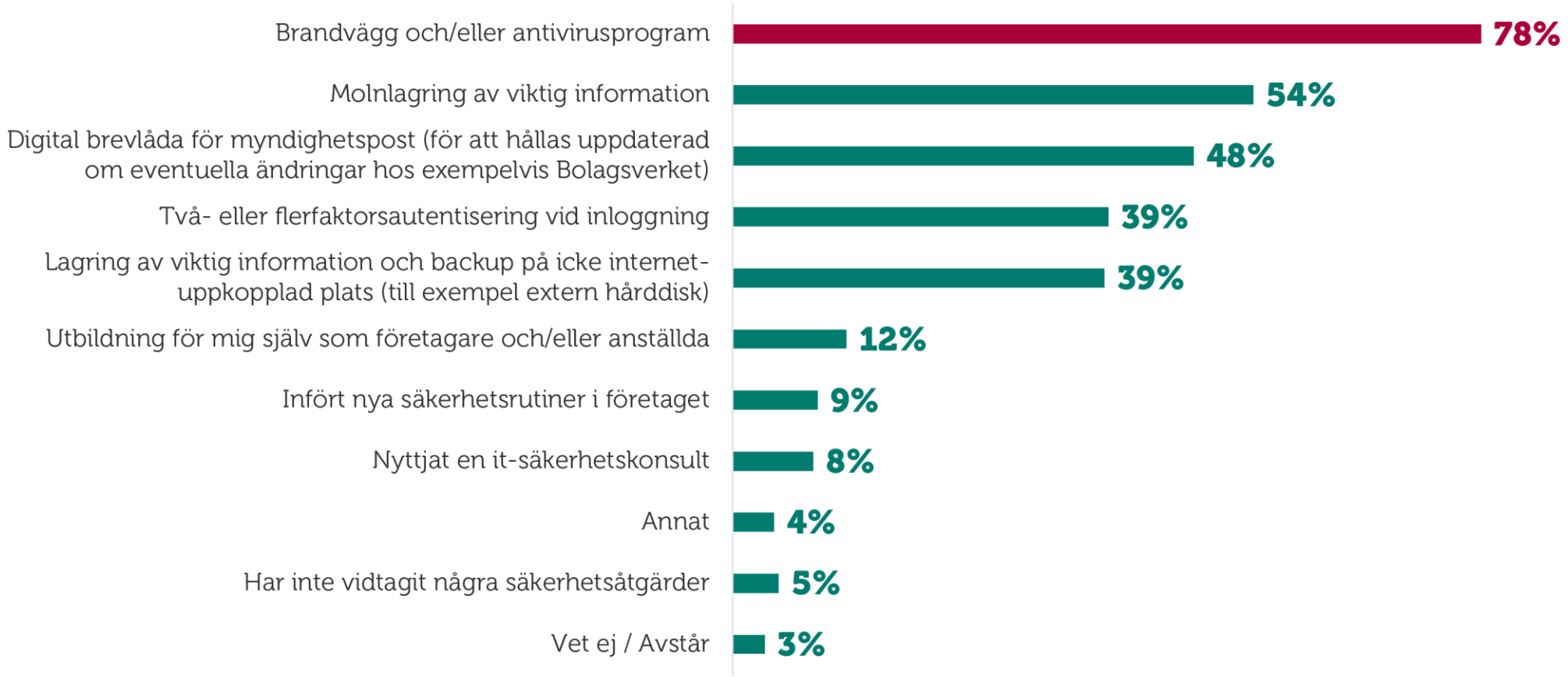
Åtgärder för att skydda företaget

- Har det upprättats en plan för incidenthantering på ditt företag, till exempel vem som ska göra vad vid en eventuell it-attack eller hur en attack kan förebyggas?
- Finns det en utarbetad policy på ditt företag för vad som ska göras vid minsta misstanke om brott från ett inkommande e-post, sms eller telefonsamtal?



företagarna

Åtgärder för att skydda företaget



Bas: Samtliga företag, n=1216.

företagarna

10 tips för ökad digital säkerhet

1. Logga aldrig in med din e-legitimation på uppmaning av någon annan om du inte själv aktivt är den som ringt upp till exempel en bank eller myndighet.

2. Installera antivirusprogram och brandvägg på företagets datorer.

3. Se till att du regelbundet gör säkerhetskopior av innehållet på din dator.

4. Tänk efter och granska kritiskt e-post innan du klickar på en länk eller öppnar en fil, även från tillsynes kända avsändare.

5. Undvik att använda publika nät.

10 tips för ökad digital säkerhet

6. Uppdatera datorn, programvarorna, mobilen och apparna med tillverkarnas senaste säkerhetsuppdateringar.

7. Lösenordet för den e-postadress som används för att återställa övriga lösenord bör innehålla många tecken och ej användas i något annat sammanhang. Spara inte lösenord i datorns webbläsare.

8. Använd tvåfaktorautentisering vid inloggning om möjlighet finns.

9. Använd en digital brevlåda för myndighetspost.

10. Ta reda på var företagets viktigaste information lagras. Dokumentera, om det behövs, rutiner som beskriver hur ni på företaget ska hantera er information säkert.

Får ingen ersättning

Plundrade e-handlaren fick negativt besked av Danske Bank

Allt fler företagare uppger att de utsatts för it-relaterade brottsförsök, som lösenordsfiske och bluffakturor. Däremot ser det mörkt ut att få ersättning från banken, ifall man lurats som juridisk person.

"Om det är företagets eller dina privata konton som tömts saknar betydelse", anser Pontus Lindström, Företagarna.

Det är en växande andel företagare som rapporterar att de utsatts för it-relaterade brottsförsök. I en undersökning, som besvarats av drygt 1 200 respondenter i Företagarnas medlemspanel, uppger tre fjärdedelar att de har varit måltavlor för kriminella som skräddarsyr bedrägerier, skickar ut virus eller hackar sig in i nätverk.

Siffran är den högsta hittills och gäller det senaste året, vilket gör den än mer uppseendeväckande, anser Pontus Lindström, Företagarnas expert på brott- och trygghetsfrågor.

Pontus Lindström, expert på brott- och trygghetsfrågor på Företagarna.

Enligt samma enkät anser sju av tio företagare att regeringen ska lägga mer krut på it-säkerhet. Även Företagarna pekar på att högerpartiernas överenskommelse lämnar en del att önska på området.

"Vi är ganska besvikna. Det saknas fokus på både it- och vardagsbrott. Den nya regeringen måste kunna hålla två tankar i huvudet samtidigt", säger Pontus Lindström och tillägger:

"Gängen ska förstås bekämpas, men de flesta brott som drabbar företagare begås inte av gängkriminella."

Det vanligaste it-brottet är lösenordsfiske, så kallad "phishing". Fler än varannan företagare uppger att de har utsatts för bedrägeriförsök via mejl. En tredjedel har fått bedrägliga sms, där syftet har varit att lura av mottagaren koder och inloggningsuppgifter.

I somras intervjuade Di företagaren Morgan Sehlstedt vars e-handel plundrades på närmare en halv miljon kronor via ett Bank-id-bedrägeri som började med ett varnande sms. Bedragarna, som utgav sig för att företräda bankens spärrservice, kom över hans kod och lyckades därigenom få tillgång till företagets konton.

Morgan Sehlstedt hoppades mycket på en vägledande HD-dom, där domstolen slog fast att Länsförsäkringar ska ersätta en kund som svindlats på närmare 400 000 kronor i ett liknande bedrägeriupplägg.

Även om frågan inte är uppklarad än finns dock signaler från jurister om att juridiska personer inte har samma ersättningsrätt som privatpersoner. Det är också beskedet Morgan Sehlstedt har fått från Danske Bank, där han är kund – både privat och i företaget. Banken har, enligt uppgift, avslagit hans ersättningskrav med hänvisning till att han lurats i egenskap av företagare.

Morgan Sehlstedt hävdar dock det motsatta och anser att han inte ska lastas för att företagets konto låg vidöppet för skurkarna som lade vantarna på hans Bank-id-kod.

"I sådana här sammanhang är det helt horribelt att inloggningen leder till både mina privata och företagets konton. Banken måste ta ansvar för att de hänger ut bolaget i min internetbank privat", säger han till Di.

Även Pontus Lindström är starkt kritisk till att företagare behandlas annorlunda.

"Naturligtvis ska det inte vara någon skillnad. Om det är företagets eller dina privata konton som tömts saknar betydelse."

Efter att Morgan Sehlstedt intervjuades i Di i augusti har flera företagare som verkar ha råkat ut för samma liga kontaktat honom. I samtliga fall har en kvinna, som påstått sig arbeta på spärrservice, varnat för misstänkt kontoaktivitet och uppmanat till kodbyte.

Ett par veckor senare, i samband med helg, har ligan slagit till och lagt upp en större mängd transaktioner till utländska konton.

Nyligen rapporterade Di om SEB:s långsamma agerande, när verkstadskoncernen Leax förkrade över 1 miljon kronor i ett så kallat vd-bedrägeri.

Ledtiden på fyra dagar, innan kontot som företagets pengar försvann in på frystes, förklarade banken med att övervakningen inte är lika intensiv på helger.

"Jag tycker att det är en rättsskandal att kriminella kan slå till på nätterna under helger utan att någon reagerar. Det är fullblodsproffs vi har att göra med. Bankerna måste vakna", säger Morgan Sehlstedt.

LINNEA BOLTER
linnea.bolter@di.se 08-573 650 21

KOMPENSERAS INTE. Morgan Sehlstedts företag plundrades på närmare en halv miljon kronor via ett Bank-id-bedrägeri som började med ett varnande sms. FOTO: STEFFAN JERNEVANG

Di den 27 och 29 oktober, samt den 3 augusti.

Fakta

Vanligaste it-brotten bland företagare

- **55 procent** har mottagit bedräglig e-post i syfte att få tillgång till personliga uppgifter, lösenord och koder.
- **35 procent** har mottagit en bluffaktura.
- **34 procent** har mottagit bedrägliga sms, också i syfte att komma över personliga uppgifter.
- **26 procent** har utsatts för virus, trojaner eller annan skadlig programvara.
- **22 procent** har blivit uppringda av en bedragare som utgett sig för att vara någon annan i syfte lura av personliga uppgifter.
- **9 procent** har utsatts för ransomware, det vill säga skadlig programvara som används i utpressningssyfte.
- **7 procent** har utsatts för dataintrång (hackare).
- **4 procent** har drabbats av identitetskapning (till exempel för att genomföra köp eller beviljas lån eller).
- **0,2 procent** har fått sina bolag kapade.

Källa: Företagarna. Frenatshträga i enkät som besvarades av drygt 1 200 företagare i organisationens företagarpanel under september. Svaren avslöjar dock inte hur stor andel av de brottsförsök man utsatts för som har "lyckats".

Juristens tips: Stresstesta bolaget för penningtvätt

Mörkertalet av företag som, medvetet eller omedvetet, hjälper kriminella pengar att bli en del av den legala ekonomin är stort. Det hävdar juristen Marie Wallin som råder företagare att identifiera svaga länkar i sina verksamheter.

Betydligt fler företag behöver få upp ögonen för hur de kan användas som en bricka i det omfattande penningtvättsmaskineriet. Det anser Marie Wallin, jurist i det egna bolaget Rätt Nu och aktuell med en handbok i penningtvätt.

"Alla branscher med kapitalvaror är utsatta. Fastigheter, bilar, båtar, konst, dyra kläder och klockor – även företag som tillhandahåller tjänster inom bolagsbildande och revision är i riskzonen."

Hon råder företagare att stresstesta sina verksamheter för att bli medvetna om hur de skulle kunna utnyttjas av kriminella.

"Fundera över hur, när och i vilken funktion ditt företag kan användas. Sök efter de svaga länkarna", säger hon och fortsätter:

"Kriminella behöver verktyg –som organisationsnummer, konton, revisorer och en verklig huvudman. En del personer utnyttjas som 'nyttiga idioter', vissa utpressas och andra saknar kunskap om hur de deltar. Lägg pusslet för att upptäcka var ditt företag skulle kunna vara en del i brottsmanuset."

Öppet köp-policyn i butiker är ett klassiskt sätt att tvätta kontanter, fortsätter Marie Wallin.

"Det kan vara ett kort som 'plötsligt strular' vid ett köp. En kompis – som uppges ha tagit emot en handpenning –dyker upp och betalar varan kontant. Efter ett par dagar återlämnas den och returen betalas in på ett konto."

"Kriminella kan tvätta tusentals kronor i olika butiker under en och samma dag. På det sättet hjälper hela samhället till att få in pengarna i den legala ekonomin."

Vad gör företag som utnyttjas sig skyldiga till?

"Blir företaget en del av kriminellas penningtvätt finns risk att enskilda medarbetare som deltagit i transaktioner hamnar i belastningsregistret. Företaget kan också åläggas en straffrättslig företagsbot."

"Det finns branscher som nästan inte rapporterar någon misstänkt penningtvätt alls till finanspolisen. Där finns troligen ett stort mörkertal, med tanke på att tröskeln för vad som ska rapporteras in är så låg", tillägger Marie Wallin.

LINNEA BOLTER

företagarna


14:01
4G
QR-kod
Om BankID
Inställningar

Tack! Frågor?

Pontus Lindström

pontus.lindstrom@foretagarna.se